PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to ensure that MDHHS creates a retrievable, exact copy of Electronic Protected Health Information (ePHI), when needed, before significant movement of equipment.

REVISION HISTORY

Issued: 09/20/2006
Revised: 01/01/2016
Reviewed: 01/01/2017
Next Review: 01/01/2018

DEFINITIONS

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Workforce Member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

POLICY

It is the policy of the MDHHS, workforce members are required to store all sensitive and ePHI on the designated network drive for their section. Workforce members shall back up all sensitive and PHI and follow established procedures to protect hard drives that contain sensitive information and ePHI in accordance with MDHHS and Department of Technology, Management and Budget (DTMB) standards.

PROCEDURE

Workforce Members

Encrypt any ePHI or other confidential information that resides on a mobile computing device that is State-owned or privately-owned

(laptops, tablet PCs, Blackberries, PDAs, etc.) according to DTMB's encryption standards.

All computing devices must have current versions of anti-virus software enabled. Operating systems must have all critical updates installed.

Position or locate workstations in a manner that will minimize the exposure of any displayed patient or sensitive business information.

When necessary, privacy screens should be used.

Employ appropriate security safeguards when accessing the MDHHS network or information from remote locations, such as connections from home.

Do not independently install connectivity hardware or software to the computing resources of MDHHS.

Comply with MDHHS and Department of Technology, Management and Budget (DTMB) policies, state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

Store all media used for backing up ePHI in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up. If an offsite storage facility or backup service is used, an appropriate written contract or Business Associate Agreement must be used to ensure that the business associate will safeguard the ePHI in an appropriate manner.

Follow established MDHHS and DTMB procedures to protect tapes, diskettes or other storage media with sensitive or PHI. DTMB Client Service Center may be reached at 517-241-9700 or 800-968-2644.

Department of Technology, Management and Budget

Equip workstations, whenever reasonable, with security that secures hardware and restricts access to software with fixed storage that support more than one user, process sensitive information or electronic protected health information, including modems.

Equip workstations, whenever reasonable with updated software for detecting the presence of malicious software (such as computer viruses).

Division Director or Section Supervisor/Manager

Establish a data backup plan to create and maintain retrievable exact copies of all ePHI determined to be medium and high risk. The data backup plan should apply to all medium and high risk files, records, images, voice or video files that may contain ePHI identified in risk assessments.

REFERENCES

45 CFR 164.310(d)(1)

DTMB 1340.00.01 Acceptable Use of Information Technology

DTMB 1340.00.170.03 Electronic Data Encryption Standard

DTMB 1340.00.110.03 Storage of Sensitive Information on Mobile Devices and Portable Media Standard

DTMB Information Technology Equipment Life Cycle (Public Act 327 of 2004 Sec. 579)

DTMB 0910.02 Records Retention and Disposal Schedules

CONTACT

For additional information concerning this policy and procedure, contact the MDHHS Compliance Office at MDHHSPrivacySecurity@michigan.gov.